Division of Archives & Records Management
Records Management Section

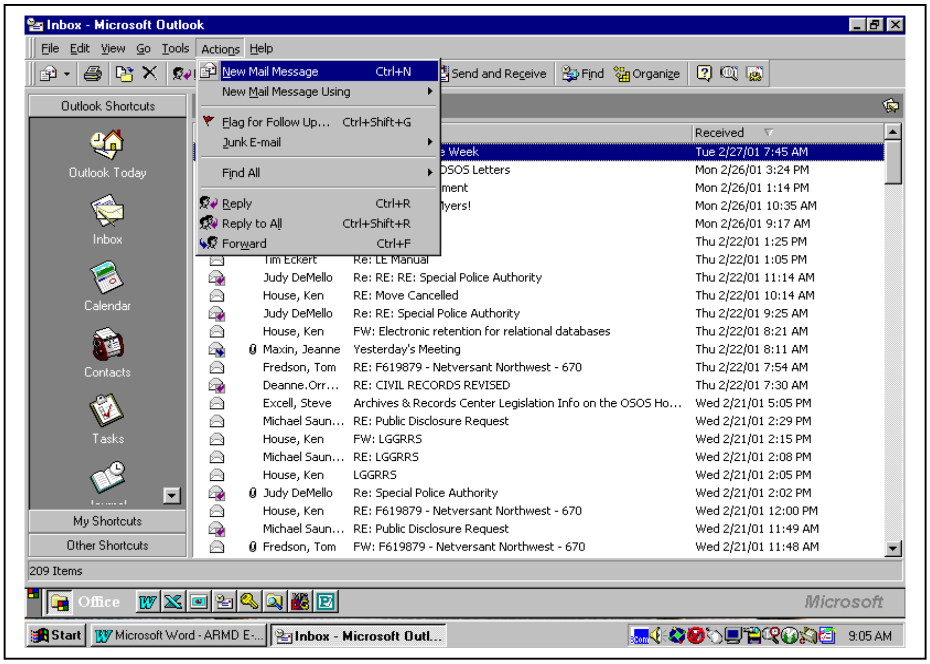
1129 Washington St.S.E.
PO Box 40238
Olympia, Washington 98504-0238

Office of the Secretary of State

ELECTRONIC MAIL

GUIDELINES FOR DEVELOPING POLICY & ESTABLISHING PROCEDURES FOR E-MAIL

A component of an agency records management program



		Received
	e Week	Tue 2/27/01 7:45 AM
	OSOS Letters	Mon 2/26/01 3:24 PM
	ment	Mon 2/26/01 1:14 PM
	lyers!	Mon 2/26/01 10:35 AM
		Mon 2/26/01 9:17 AM
		Thu 2/22/01 1:25 PM
Tim Eckert	Re: LE Manual	Thu 2/22/01 1:05 PM
Judy DeMello	Re: RE: RE: Special Police Authority	Thu 2/22/01 11:14 AM
House, Ken	RE: Move Cancelled	Thu 2/22/01 10:14 AM
Judy DeMello	Re: RE: Special Police Authority	Thu 2/22/01 9:25 AM
House, Ken	FW: Electronic retention for relational databases	Thu 2/22/01 8:21 AM
Maxin, Jeanne	Yesterday's Meeting	Thu 2/22/01 8:11 AM
Fredson, Tom	RE: F619879 - Netversant Northwest - 670	Thu 2/22/01 7:54 AM
Deanne.Orr...	RE: CIVIL RECORDS REVISED	Thu 2/22/01 7:30 AM
Excell, Steve	Archives & Records Center Legislation Info on the OSOS Ho...	Wed 2/21/01 5:05 PM
Michael Saun...	RE: Public Disclosure Request	Wed 2/21/01 2:29 PM
House, Ken	FW: LGGRRS	Wed 2/21/01 2:15 PM
Michael Saun...	RE: LGGRRS	Wed 2/21/01 2:08 PM
House, Ken	LGGRRS	Wed 2/21/01 2:05 PM
Judy DeMello	Re: Special Police Authority	Wed 2/21/01 2:02 PM
House, Ken	RE: F619879 - Netversant Northwest - 670	Wed 2/21/01 12:00 PM
Michael Saun...	RE: Public Disclosure Request	Wed 2/21/01 11:49 AM
Fredson, Tom	FW: F619879 - Netversant Northwest - 670	Wed 2/21/01 11:48 AM

How to be an effective Records Manager
Records Management Informational Pamphlet – MARCH, 2001

GUIDELINES FOR DEVELOPING POLICY & ESTABLISHING PROCEDURES FOR E-MAIL

Table of Contents

GUIDELINES FOR DEVELOPING POLICY & ESTABLISHING PROCEDURES FOR E-MAIL

Introduction

Electronic mail (e-mail) is one tool that is helping organizations change the way they conduct business. E-mail provides a means to create, transmit, and respond to messages electronically. An increasing number of state agencies use e-mail systems to distribute memos, circulate drafts, disseminate directives, transfer official documents, and send external correspondence that support various aspects of business operations.

Well-designed and properly managed e-mail systems expedite business communications, eliminate paperwork, and automate routine office tasks. However, the opportunities for cost savings and increased efficiency are lost if e-mail systems and the electronic documents they handle are not managed effectively. Personal use of e-mail, loss of control over public records, increases in trivial and duplicate messages, and concerns about privacy, security, and public access can offset the benefits of e-mail.

Records in e-mail systems can be managed successfully through a combination of policies, system design, management procedures, and end user training. This publication provides practical guidance so agency records managers can work together with their agency program managers, network administrators, and end users to better ensure that e-mail messages, like other records, are identified, made accessible, and retained as long as needed to satisfy record-keeping requirements.

Electronic Mail Definitions

Electronic mail or e-mail is an information transfer system, which uses computers for sending and receiving messages.

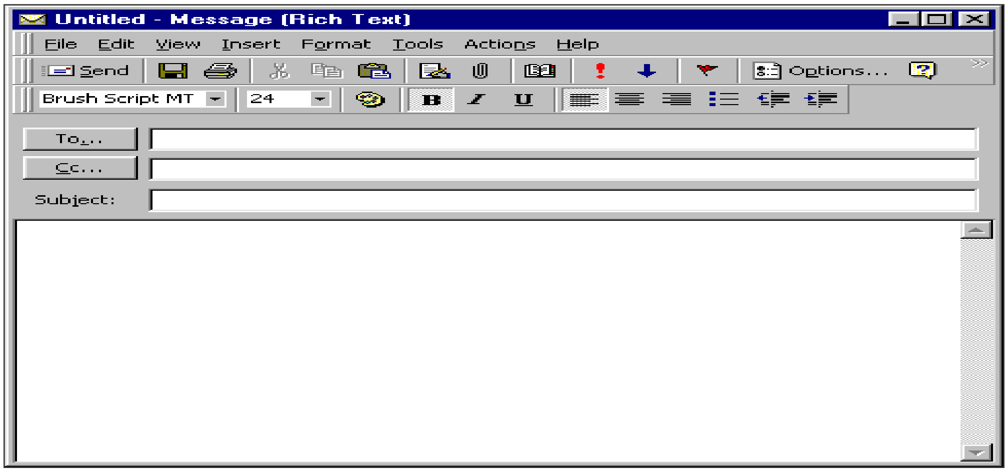
E-MAIL SYSTEMS

The electronic mail **system** provides the means for creating messages, transmitting them through a network, and displaying the messages on the recipient's workstation, personal computer (PC), or terminal. E-mail systems can provide an array of features including graphical user interfaces, advanced editing and document management capabilities, secure transport services, directories of user addresses, and message authentication. They are storage and deliver software systems that transport messages from one computer user to another. E-mail systems range in scope and size from a local area network e-mail system that carries messages to users within an agency or office; to a wide area in various physical locations; to Internet e-mail systems that allow users to send and receive messages from other Internet users around the world.

E-MAIL MESSAGES

E-mail **messages** are electronic documents created and sent or received by a computer system. This definition applies equally to the contents of the communication, the transactional information and any attachments associated with such communication. Thus, e-mail messages are similar to other forms of communicated messages, such as correspondence and memoranda. E-mail messages consist of individual units of information divided into an “envelope” and the message contents. The envelope, also called the “message header,” contains the mailing address, routing instructions, transmission and receipt data, and other information the system needs to deliver a mail item correctly. Most e-mail systems allow senders to attach documents to messages, import text from word processing systems to e-mail applications, forward messages, and distribute information to individuals and groups. More sophisticated e-mail applications include workflow software that manages the movement of messages, forms, and documents through a work group or organization.

Figure 1 - Components of an E-mail Message


Untitled - Message (Rich Text)
File Edit View Insert Format Tools Actions Help
Send
Options...
Brush Script MT
24
B I U
To...
Cc...
Subject:

Are E-mail Messages a Public Record?

Yes, all e-mail messages using state government systems that are sent or received, that contain information about business activities, and that can function as evidence of business transactions are, regardless of recorded medium, part of the records of the agency and must be managed in accordance with the General Records Act Chapter 40.14 RCW. They are also subject to related legislation such as the Public Disclosure law Chapter 47.12 RCW, Essential Records Chapter 40.10 RCW and Penal provisions Chapter 40.16 RCW. Consequently, all e-mail messages that are public records are subject to record retention requirements. For the purpose of satisfying public record laws, e-mail is defined as not only the messages sent and received by e-mail systems, but all transmission and receipt data as well. Courts have accepted e-mail as a legitimate source of evidence and it is therefore subject to legal processes such as subpoena.

Challenges of Managing E-mail Records

One of the greatest challenges of managing e-mail effectively is to ensure that all records, which originate or are transmitted through the system, are identified, retained, and managed properly. Records should be readily available and accessible to all authorized users when they need them and in a useable format. This means that the identity, purpose, and location of records are predictable, consistent, and reliable; methods for access and retrieval are simple and well defined; and records management practices are incorporated into day-to-day business activities.

Public records should be segregated from transitory messages that do not document agency business, extra copies of documents, and drafts that do not reflect substantive changes. Because e-mail is easy to use for both formal and informational communications, the proliferation of informal and transitory messages that do not provide evidence of official policies and transactions is a common problem in e-mail systems. These administrative materials with no retention value do not warrant the same degree of control, security, or protection afforded to public records, and they accumulate rapidly in e-mail systems.

Basically, the content and not the medium determine the treatment of the message. E-mail records, like other agency records, must be classified within the appropriate record retention schedule. For instance, all e-mail may be considered correspondence, but may include attachments such as reports, contracts, accounting records and so on.

Types of messages sent by e-mail that typically are records:

- Policies and directives
- Correspondence or memoranda related to official business
- Work schedules and assignments
- Agendas and minutes of meetings
- Drafts of documents that are circulated for comment or approval
- Any document that initiates, authorizes, or completes a business transaction
- Final reports or recommendations

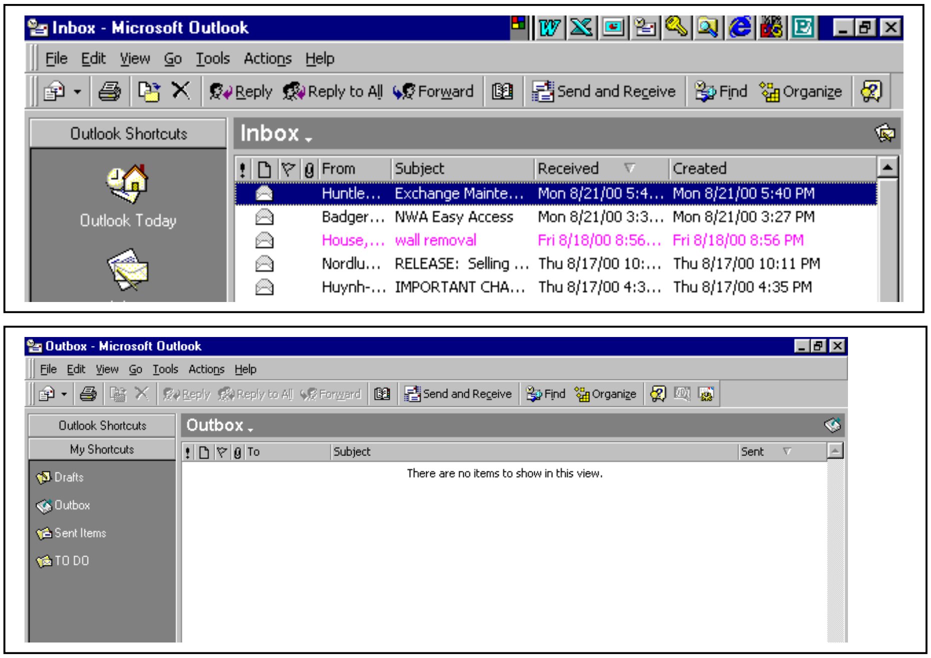
Types messages sent by e-mail that typically have no retention value (see General Schedule 50 001. Having no retention value means may be destroyed when no longer needed.

- Personal messages[1] and announcements not related to official business
- Information-only copies or extracts of documents distributed for convenience of reference
- Published reference materials
- Copies of inter- or intra-agency memoranda, bulletins or directions of a general information and non-continuing nature
- Announcements of social events, such as retirement parties or holiday celebrations.

[1] Personal messages may contain evidence or historical material – contact your agency records officer to determine evidence or historical value.

Typically, E-mail system utilities do not distinguish public records from messages that are not records.

Figure 2 - Typical E-mail Inbox and Outbox.



!				From	Subject	Received	Created
				Huntle…	Exchange Mainte…	Mon 8/21/00 5:4…	Mon 8/21/00 5:40 PM
				Badger…	NWA Easy Access	Mon 8/21/00 3:3…	Mon 8/21/00 3:27 PM
				House,…	wall removal	Fri 8/18/00 8:56…	Fri 8/18/00 8:56 PM
				Nordlu…	RELEASE: Selling …	Thu 8/17/00 10:…	Thu 8/17/00 10:11 PM
				Huynh-…	IMPORTANT CHA…	Thu 8/17/00 4:3…	Thu 8/17/00 4:35 PM

!				To	Subject	Sent

There are no items to show in this view.

Establishing E-mail Policies & Procedures

Agency policies should establish general guidance on the use of e-mail to conduct official business, on access and privacy protection of e-mail messages, and on management and retention of e-mail. Policies should also define the roles and responsibilities of end users, managers, technical staff, records management staff, and support staff because traditional roles and responsibilities are changing as new technologies are introduced into the workplace.

Policies will help staff use e-mail properly, consistently, and effectively; reduce the risk of loss, corruption, mismanagement, and unauthorized access to e-mail messages; and increases the quality and value of agency records. Existing policies for telephone, fax, or written communications may not address all issues raised by e-mail, because e-mail combines some characteristics of electronic communications with elements of written documents. Because most agencies create and receive records in both paper and electronic formats, management of paper and electronic records must be coordinated to avoid gaps in documentation, inconsistencies, or unnecessary duplication. Agency e-mail policies should effectively address the following:

APPROPRIATE USE OF E-MAIL

Agencies provide e-mail services, like other means of communication, to support official business. Therefore, policies should define proper use of e-mail and set limits on personal use. Agencies may set the same strict limitations on personal use of e-mail that exist for telephone, fax, and postal mail; or, recognizing that some personal communications are likely, they should permit internal personal use within specific limits, such as to announce work-related social events.

Essentially all e-mail users are responsible for appropriate use of e-mail and for certain aspects of the management of records in the e-mail systems. Users should be informed of their responsibilities to:

- Limit their use of the e-mail resources to official business
- Respond promptly to messages
- Protect e-mail messages, files, and records from unauthorized release to third parties
- Remove personal and transitory messages from personal in-boxes on a regular basis and regularly transfer public records to an organized, secure, and accessible filing system
- Protect e-mail messages from inadvertent loss or destruction by complying with backup requirements and procedures
- Coordinate disposition of public records with the agency Records Management Officer to ensure that retention requirements are met.

PRIVACY PROTECTION

Agency e-mail policies must comply with the laws relating to disclosure and confidentiality issues. On April 25, 2000 Governor Gary Locke sent Executive Order 00-03 Public Records Privacy Protections Preamble to State Agencies. The order made critical distinctions between public information and private personal information that is held by government business. The order was specific on limiting the collection and retention of personal information. It specifies the need to identify and to protect any system of records that contains personal identifiable information and retaining such information only as long as needed to carry out the purpose for which it was originally collected, or the minimum period required by law.

EMPLOYER'S RIGHT TO ACCESS

Agencies have an obligation to inform users about the terms and conditions under which requestors may be granted access to e-mail, as well as the responsibilities of end users to protect the personal privacy of individuals who may be subjects of e-mail messages. According to the Federal Electronic Communications Privacy Act (ECPA) of 1986, e-mail users have a reasonable expectation of privacy protection for their mail. An important exception to ECPA grants employers the right to intercept, monitor, and read employee communications as long as those are done in the ordinary course of business and for a legitimate business purpose. Policies should inform users that e-mail messages sent or received in conjunction with government business:

- May be accessed and monitored in the normal course of business by system administrators, supervisors, and support staff
- May be releasable to the public
- May require special measures for privacy protection
- Are subject to discovery proceedings in legal actions.

Retention and Scheduling Requirements

E-mail itself is not considered a record series or category. It is a means of transmission of messages or information. Like paper or microfilm, e-mail is the medium by which this type of record is transmitted. Just as an agency cannot schedule all paper or microfilm records together under a single retention period, an agency cannot simply schedule e-mail as a record series. Rather, retention or disposition of e-mail messages must be related to the information they contain or the purpose they serve. The content, transactional information, and any attachments associated with the message are considered a record. The content of e-mail messages may vary considerably, and therefore, this content must be evaluated to determine the length of time the message must be retained.

Simply backing up the e-mail system onto tapes or other media or purging all messages after a set amount of time is not appropriate strategies for managing e-mail.

E-mail records should be kept for the retention period identified on either the state's general records retention schedule or an agency specific schedule. The retention periods apply regardless of the record's medium or method of transmission; the content determines how long the record will be maintained

As previously discussed, the management and retention of e-mail records are subject to state records management laws and regulations. Agency policies should inform e-mail users that public records communicated through e-mail systems must be identified, managed, protected, and retained as long as needed for ongoing operations, audits, legal proceedings, research, or any other known purpose.

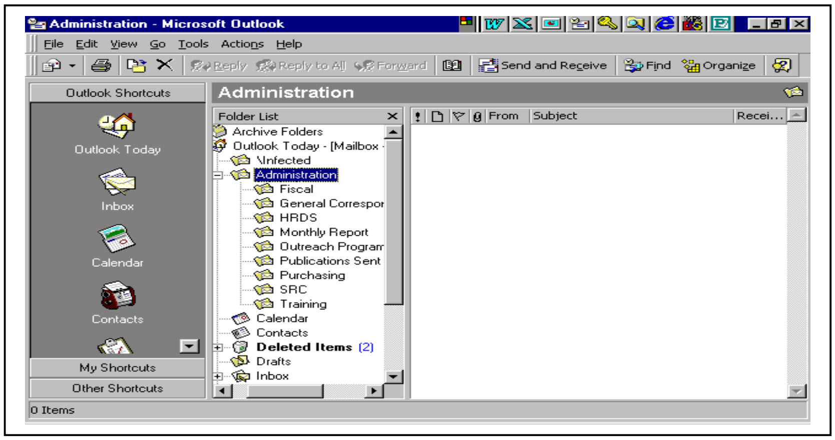
DETERMINE WHO HOLDS THE PRIMARY RECORD COPY

E-mail users should be aware that e-mail messages are often widely distributed to a number of various recipients. Determining which individual maintains the primary record copy of the message, i.e. the original message that must be retained per the retention schedule, is vital to e-mail management. If the holder of the record copy is not identified and aware of his/her responsibility, the agency may find that no one retains the message or that everyone retains the message. Neither of these scenarios is appropriate.

EXAMPLE: Copies of agency policy documents that are transmitted to multiple recipients. Each recipient need not retain the document beyond his or her need for this information provided an office or agent establishes the record copy responsibility for its established retention period. In this example, the logical record copy responsibility rests with the creator of the policy document. *Prompt deletion of duplicate copies of e-mail messages from an e-mail system makes the system much easier to manage and reduces disk space consumed by redundant information.*

Generally speaking, the individual who sends an e-mail message should maintain the record copy of the message. However, the varied uses and wide distribution of e-mail may result in many exceptions to this rule that will have to be dealt with internally.

DETERMINE BEST METHOD FOR FILING AND STORAGE



Your mail system usually has the option of creating other “mailboxes” or “folders”. After brief periods in your Inbox, messages should be transferred to other boxes, based on business and retention requirements. *Employees should be responsible for classifying messages they send or receive according to the content, the agency’s folder/directory structure and established record series*

Use subject lines on your e-mail both to help you and the recipient identify and file messages. Subject lines should be descriptive as possible (example: “quarterly financial report” no “report”, or “August, 2000 State Records Committee Minutes” not “minutes”, “potluck today” not “today’”).

We recommend that agencies explore three options when retaining records from an email system: on-line storage, near-line storage, and off-line storage. Each of these options carries with it benefits and disadvantages and may be affected by your agency's information technology environment. It is important to remember that messages only have to be retained and stored for as long as the retention period requires. Very few messages must be maintained for a long period of time or permanently. The storage method of e-mail may also depend on the retention period of the record. Messages that need to be retained for six months should be relatively easy to maintain on the current mail system and then delete. Storage decisions for messages that are designated Archival or long-term need will require careful consideration.

On-line storage is defined as storage of email messages, metadata[2], and attachments in an email system, which is being used at an agency. The system in use does not necessarily have to be the same throughout the retention.

On-line storage maintains the full functionality of the email message, and allows users to recall the message at any time for reference or responding. A *disadvantage* of on-line storage is the potential cost and effect of storage on the performance of the email system. Any solution to email retention, which includes on-line storage, should be done only after consultation with the agency information resource manager and the agency network administrator.

[2] *Metadata is defined as the data about the data that are contained in a data resource directory or a data directory.*

Near-line storage is defined as storage of email messages, metadata, and attachments in an electronic record keeping system. This type of storage requires that the message, metadata, and attachments be removed from the on-line email system and stored in an electronic format. For example, a message stored in an on-line email system can be saved to a file on a local hard drive. The file should be stored in a format that is compatible with agency operations, and filed according to filing practices established by the agency and/or user.

Near-line storage allows the user to maintain a moderate amount of functionality, in that email messages stored near-line can be retrieved and referenced electronically. In storing e-mail messages, metadata, and attachments, users should be careful to maintain a filing system that is consistent with established practices. This includes filing sequences as well as the use of naming conventions for computer files. In addition, users may want to consider "protecting" such records from alteration.

Off-line storage is defined as the storage of email messages, metadata, and attachments outside of an electronic record-keeping environment. The clearest example of this type of storage is to simply print out an email message to paper, with its contextual information and attachments in place, for filing within existing filing systems in the agency.

Off-line storage reduces functionality dramatically in that; email messages are no longer retrievable in electronic format. However, off-line storage offers users the ability to integrate the filing of records in email systems within existing hard copy filing systems in agencies. Any email messages, metadata, and attachments stored off-line should be done in a manner consistent with agency practice.

The State Archives only accepts archival records in paper, microform, and audio-visual formats. Planning and provision for archival or other long-term retention should be part of the design of any record-keeping system. The technology necessary to retrieve the records in an intelligible form from their physical carrier changes at a faster rate than the carriers themselves deteriorates.

For example, in computerized systems, records come into being through transactions that occur within and between systems and the interaction of both hardware and software. Such records will not necessarily continue to be retrievable over extended time merely because their component parts are stored on any particular medium. Access to or retrieval of electronic records created in specific environments will usually require a capacity to replicate those measures at a later time to ensure authentic versions of records are available, even though the technical retrieval process may be different.

It would be very expensive for State Archives or an agency to duplicate every possible configuration of software and hardware that might at any time have been in use within any one agency as a whole. To maintain generations of obsolete software and hardware as well as the technical expertise and environments would be extremely difficult to justify logically, practically and economically. Such an approach would result in wasteful expenditure of resources by the State Archives or an agency, without any assurance that the records concerned would continue to be accessible or retrievable when required for the future.

We recommend that archival or those records requiring a long-term need (10 years or greater) should use the off-line storage method.

SECURITY

Adequate system security is necessary to protect records transmitted by e-mail against inappropriate or unauthorized access, actions that might compromise the accuracy and authenticity of records, and damage or loss in the event of a system failure or natural disaster.

Protecting records in computer systems begins by identifying potential threats to the system. These threats may be intentional or unintentional, including:

- Physical threats to buildings and computer facilities
- Natural disasters and environmental threats
- Computer hardware and software failures
- Media vulnerabilities
- Communications vulnerabilities
- Human error

Although use of computer networks increases the vulnerability of electronic records, there are a number of ways to protect data and records in a network environment. The appropriate strategy and level of security depends on the risks involved, the value of records and data, and the costs at stake in the event of temporary or permanent loss. To ensure the security and authenticity of records communicated through e-mail systems, networks and e-mail applications must have access and security controls that restrict who can read, write, change, and delete files. Today's networking and e-mail systems offer many options for supporting controlled, secure, and reliable communications.

Password protection restricts access to a system or application to authorized users. Use of passwords in an e-mail system is the shared responsibility of network administrators and e-mail users. In order to ensure that records in e-mail are protected and maintained in a secure manner, users should

- Choose passwords that are difficult for people or computer programs to guess
- Refrain from sharing or disclosing their passwords
- Keep track of previous log-ins to detect unauthorized access
- Change passwords the first time they log in and on a regular basis thereafter.

Network administrators can further restrict access privileges to specific individuals who are authorized to participate in a business process by limiting rights to create, send, or alter messages in specific directories, subdirectories, or files.

Message protection and authentication controls prevent users from changing an e-mail message once it has been received by at least one recipient. These controls require users to send a new message with new transmission and receipt data if they wish to change the content of the message. This feature supports authentication and version control of electronic documents.

The sender can attach security, special handling labels such as such as urgent, confidential, or acknowledgement requested, to an e-mail message.

System audit trails automatically record the circumstances surrounding login attempts, creation, transmission and receipt, filing and retrieval, updates, and deletion of messages in an e-mail application or on a network. Even the best-designed security measures are vulnerable to intrusion by determined culprits. Therefore, system administrators should design and use audit trails that monitor a system's performance, ensure that security procedures were followed, and audit the transmission of messages in the system. Other security measures such as encryption, virus protection, and backup procedures provide additional protection against unauthorized access, alteration, or loss of records. Security measures can be costly to design, enforce, and monitor. Program managers and network administrators should work together to assess risks and design security measures that are commensurate with the degree of risk associated with each system or application.

E-MAIL MESSAGES AND THE RULES OF EVIDENCE

Agency personnel should be familiar with both state and federal "rules of evidence" requirements. For records maintained in electronic information systems, including e-mail systems, courts concentrate on assurances those records, and the systems in which the records are created and maintained, are reliable. The reliability of the process or system used to produce records, not the type of media or technology used, determines the admissibility of records in evidence. Moreover, the federal rules of evidence place the burden for the identification of relevant records on the record creator, and often within a ninety-day time period. At a minimum, agency personnel should ensure the following:

- E-mail systems used to create, receive and maintain e-mail messages have full, complete, and up-to-date systems documentation
- E-mail systems follow all recommendations for system security
- Complete systems backups are regularly and consistently performed
- E-mail system retains all data and audit trails necessary to prove its reliability as part of the normal course of agency business
- The record copy of a message is identified and maintained appropriately
- Backup procedures should be coordinated with disposition actions so that no copies of records are maintained after the retention period for the records has expired

Agency records officers need to plan for records maintenance and record copy responsibilities for the records system to meet requirements for reliability and legal records disposition.

The e-mail system should allow the server administrator to prevent destruction of records for legal and/or audit purposes.

ACCESSIBILITY

A major challenge for agency records officers is to guarantee that records maintained in electronic information systems are accessible and usable for the entire length of the retention period. Rapid changes and enhancements to both hardware and software compound this challenge. As many e-mail systems have limitations in storage space that cause operational problems when messages are stored in the system beyond a specific period (such as sixty or ninety days), procedures must be in place to transfer records from the e-mail system to another electronic records keeping system to meet retention requirements. Again, it is illegal in Washington to destroy a public record, including records created in an email system, without a formal retention period being established for the record through an authorized records retention schedule, and without following records disposition procedures.

Messages should be maintained in a format that preserves contextual information (metadata) and that facilitates retrieval and access. The system should allow deletion of messages once their retention periods expire.

Beyond this generic challenge of technology change, there are more mundane, but equally critical steps that must be in place to ensure that records created by e-mail systems can be located and retrieved when required. A central step is a system of standardized naming conventions and filing rules within the e-mail systems. E-mail messages should be indexed in an organized and consistent pattern reflecting the ways in which records are used and referenced. Records maintained electronically, including e-mail messages, have an advantage over conventional “hard copy” document filing systems in that indexing for multiple access points is relatively simple and inexpensive, provided an effective indexing framework is in place. Planning records indexing and retrieval points is time well spent. Unnecessary time needed to retrieve electronic records is not productive staff time, and is an annoyance to the public as well. Messages should be stored in a logical filing system that is searchable by multiple data elements.

In an effort to assist agencies in developing solutions to this issue, standard practices for establishing directories, defining documents, and naming files will facilitate the management of e-mail records in an electronic filing system. Conventions in the following areas will facilitate access, retrieval, and sharing of electronic records.

Naming conventions for business functions, applications, file classifications (folders), documents, and document types support accurate filing and consistent retrieval of records. Naming conventions help users organize incoming and outgoing messages and decide where to route or file e-mail messages. Consistent use of naming conventions also enables automatic routing, sorting, filing, and deleting of e-mail.

USER TRAINING AND SUPPORT

User training and support is an essential ingredient in any effective system. Many agencies provide training and support to help staff use application software and other technology tools appropriately and effectively. As agencies rely increasingly on e-mail systems to support official agency business, all users should be able to identify records in e-mail applications and know what their responsibilities are for managing, maintaining, protecting, and providing access to them. Users should also be informed about the legal and audit requirements associated with records. Formal training sessions offer a forum for informing users about their records management responsibilities and for demonstrating software tools that support effective records management.

BIBLIOGRAPHY

University of the State of New York, State Education Department, State Archives and Records Administration, *E-mail Systems and Records,* 1999.

University of the State of New York, State Education Department, State Archives and Records Administration, *Managing Records In Automated Office Systems*, 1990.

Indiana Commission on Public Records, Electronic Mail Retention Guidelines, 1999

Delaware Public Archives, Appendix Q Policy Statement and Guidelines – Electronic mail, 4/1999.

Maine State Archives, Electronic Mail and Voice Mail: A management Guide for Maine State Government, 11/1998

State of Ohio Managing Electronic Mail, 2/2000

APPENDIX A

Frequently Asked Questions about e-mail Retention

1. **Can I print messages, and then delete them?** Yes, provided you print the following information with the message: name of sender, name of recipient, date and time of transmission and/or receipt. You then retain the printed message according to the appropriate record retention schedule, file them as suits your business needs, and destroy or transfer them to the Archives, depending on the schedule.

2. **What about draft documents that undergo several revisions?**
Draft documents or working papers that are circulated via e-mail, that propose or evaluate high-level policies or decisions and provide unique information that contributes to the understanding of major decisions of the agency should be preserved according to the appropriate retention schedule. Other drafts circulated for comments, which demonstrate significant revisions in the view of the author, should be scheduled, as is the final product. Un-circulated drafts may be destroyed at will by the author.

3. **What do I do with attachments I receive with e-mail?**
File them with other electronic documents on your PC or network and apply the appropriate retention schedule. The principles of directory and file organization used in e-mail should be followed for content files (documents, databases, and spreadsheets). Example: you have a PROJECTS\WORKFLOW\2000 folder in your e-mail system and probably should have a similar one for related PC files. Attachments relevant to that project can be transferred to that directory.

4. **What about multiple copies of the same document?**
If another agency or office has the primary responsibility for keeping the record copy, and if you have no business need to retain it, the document is simply an informational copy and subject to deletion/destruction at will. Example: If you receive the minutes of a meeting that provide you with the authority to travel to a far away place for a special seminar, definitely incorporate it into your project files. Otherwise, when you receive minutes of a meeting you attended as an informational copy, may be destroyed at will. The secretary or other responsible person in the organization, committee or task force must retain the minutes per their retention schedule (such as GS 10004 or GS09009).

5. **Do I need to keep distribution lists?**
If you send to a distribution list, you must also keep a copy of the members of that list for as long as you are required to keep the message itself.

6. **How do I get a copy of my office record retention schedule?**
Contact the records coordinator for your office or your agency records officer. If you don't know who your agency records management officer is, contact the Records Management section of the Washington State Archives: *(360) 586-4902* or dcasler@secstate.wa.gov.

APPENDIX B

A Guide to E-Mail Etiquette[3]

Know your audience.
Be aware of the culture and conventions of your e-mail recipients. Communication and especially e-mail conventions may vary between groups. Remember that different users have different levels of experience with technology applications like e-mail. Be patient and supportive with new users

.

Proofread.
Spelling and grammar mistakes can be just as distracting in an e-mail message as they are in written communications. Take the time to proofread your messages, especially messages that are used to communicate or document agency business.

Keep messages brief and to the point. Make your messages “concise” not cryptic. Shorter paragraphs have more impact and are more likely to be read by busy people. Most people can only grasp a limited number of ideas within a single paragraph, especially on a computer screen.

Format messages for easy reading.
White space enhances the look and clarity of an e-mail message, and blank line only ads a byte to the message so do not be stingy. Lengthy messages are almost always read in hard copy form and should be prepared accordingly (e.g., with cover sheets, headers, page numbers and formatting).

Do not over-distribute e-mail.
Every message you send creates work for someone else who must read, consider, and deal with the message. It may be better to post some messages on an electronic bulletin board in order to reduce the number of copies routed to individual users.

Respect the privacy rights of others.
Do not invade privacy. Do not forward or distribute messages without permission. Do not read other people’s mail. If you receive someone else’s mail, e.g., because the sender entered a wrong address or you happen upon a PC or terminal someone failed to log-off of, use the same consideration you would with traditional mail. Informs the appropriate party, see that the mail is returned, and notify your network administrator

Be aware of differences across e-mail systems.
Others may not have the same e-mail features or capabilities you have, in which case, avoid special control characters like bold, underline, and special fonts; even tabs can differ. With the exception of binary (program) files, keep your lines under 80 characters; if possible do not exceed 72 characters. Be sure that your editor inserts carriage returns at the end of each line if not, enter a hard return. Be extra careful with graphics. Whenever possible, find out in advance what e-mail features and software tools your recipients have.

[3] *This Guide to e-mail Etiquette incorporates conventions and similar guidelines compiled by:*
Gargano, Guide to Electronic Communication and Network Etiquette*, (1989); Goode and Johnson, "Putting Out the Flames: the Etiquette and Law of E-Mail."* ONLINE*, (1991); Krol,* The Whole Internet User's Guide and Catalog*, (1992); and Robinson,* Delivering Electronic Mail*, (1992).*

Cite the appropriate references and context of a message.
Reference any related e-mail message or posting, and the event, topic, or issue that your message refers to, in order to avoid being taken out of context and misinterpreted. Take the time to back up your statements with references to documents or articles just as you would in written material.

If a message is referencing an earlier note, include enough of the original message to make the message clear.

Identify yourself.
Especially if you are acting on behalf of an organization or professional association, or if you have relevant background or expertise in a matter, identify your affiliation, title, background and expertise in your e-mail message. Include your e-mail address in the message and any attachments to it.

Separate opinion from non-opinion.
So that readers do not confuse personal opinion with agency policy or position, use labels and explanatory notes to distinguish opinion from fact. If necessary, include a brief disclaimer.

Respect copyright and license agreements.
Copyright laws are applicable to e-mail networks. Some software that is available for public retrieval through the Internet requires a valid license from the vendor in order to use it legally. Posting information on networks is similar to publication. Be careful to cite references.

Label messages that are meant to be humorous and be careful with sarcasm.
Use established conventions or explanatory notes to alert the recipient that a message is meant to be taken humorously. Facial expressions, voice inflection and other cues that help recipients to interpret a message are absent from e-mail. You cannot always control when and in what context a message will be read. The wrong party might read it at the wrong time or. The reader might not understand your intention.

Avoid sending e-mail in anger or as an emotional response.
It is best not to send these kinds of messages over e-mail. Such situations are better worked out in person or in another forum. If you do send such a message, be sure to warn readers of your intent with the use of established conventions or explanatory notes. (These messages are often called *"flames"*.)

Do not be hasty.
If a message or posting generates negative feelings, set it aside and re-read it later. An immediate response is often a hasty response. Do not rule out the possibility that a misunderstanding or misinterpretation might occur. This is common with e-mail because of the lack of physical cues.

Avoid putting text in all capital letters.
Most users suggest that you avoid putting all text in caps because it may seem ANGRY or HARSH. Upper-case text is often interpreted as having extra emphasis.

Be careful what you say about yourself and others.
As a general rule of thumb, do not commit anything to e-mail that you would not want to become public knowledge. Think twice before posting personal information about yourself or others. There is always the chance that a message could end up in someone else's hands. Be aware that e-mail messages are often retained on system backup tapes and disks in central computing facilities after they are deleted from the mail system.

Do not be fooled by the illusion of privacy.
Assume that your message could be around for a long time. It is easy to copy, store (electronically or in hard copy), resurrect, and forward anything you write in e-mail.

Do not send abusive, harassing, or bigoted messages.
This is inappropriate and counter-productive for obvious reasons and reflects badly on the individual and the entire organization. Even on wide area networks, e-mail can usually be traced to the originating machine and user. Systems on the Internet are actually liable for the misdeeds of their users.

Re-read your mail for content and tone before you send it.
On many systems, once you send a message you are committed to it, and cannot retract it.

Try to keep messages to a single subject; use subject entries.
The subject line of an e-mail message serves a number of important purposes: (1) it enables busy people to discern the subject of a message and when it must be read; (2) it is used to index the message in mailboxes and file folders; (3) it may be used to identify what messages are "records" and need to be transferred to a central record-keeping system in the agency.

Only post messages when they are relevant.

Do not make messages "urgent" when they do not need to be.
Most of us learned the lesson of *"the boy who cried wolf"* quite some time ago. In today's world, this lesson rings true for the misuse of priority mail notices. These notices will soon become meaningless with overuse.

APPENDIX C

SAMPLE E-mail Policy/Procedure

Agency Name
Policy/Procedure

Title	Electronic Messaging Systems Use and Privacy	Number: 10.005
References:	RCW 42.17, 40.14;	
Contact:		
Effective Date:	February 2002	
Supersedes:		
Approved		
	Secretary, Agency Name	

Purpose:

This policy defines the framework for use of electronic message systems and communications media by employees of the AGENCY NAME. This includes but not limited to, electronic mail systems (e-mail), voice mail systems, calendar scheduling systems, faxes, Internet and other electronic media that generate, store, transmit and display correspondence for internal and external business communication purposes.

Definitions:

- Communications is defined as a system for sending and receiving messages, as by mail and telephone.
- Media is plural of medium that is defined as an agent by which something is conveyed, accomplished, or transferred.
- Communications media is that aspect of electronic messaging systems that contains the message.
- Employee is a person who is a permanent, temporary, contractor, and student intern employee or otherwise engaged at the agency and has been given authorized access to any agency electronic messaging system.
- Encryption is a method of “scrambling” data using a cryptographic algorithm based on a secret key that is known only to the originating system and the destination system.
- Securing a device means to log off the network, invoke a keyboard-locking feature requiring a password, or otherwise makes the device inaccessible.

Policy:

1. **The Department will provide electronic messaging systems, making them available to agency employees as required subject to resources and other limitations. Employees with assigned access to electronic messaging systems are expected to use them.**
   - The Secretary, Assistant Secretaries and members of their management teams are expected to use the department calendar scheduling system.
   - Employees with access to electronic messaging systems are expected to check for messages on frequent and regular basis and respond within a reasonable time as needed.

2. **Department-owned electronic messaging systems will provide data confidentiality and integrity. Employees must use reasonable means to minimize unauthorized access to electronic messages.**

   - Employees are responsible for protecting messages from unauthorized access by maintaining password confidentiality and by securing the communications device to the extent possible before leaving it unattended.
   - Confidential and sensitive written information must be encrypted before transmitting electronically. This applies to information sent within the department and especially to information sent to external agencies.

3. **An employee's use of state-provided communication media is restricted.**

   - Employees are expected to use state-provided communications media only for state business**.** However, the department recognizes the occasional need to exchange personal messages. At no time should personal messages be sent in a way the charges the state for transmission.
   - Employees shall not use state-provided communications media in a fashion that constitutes or involves any unlawful activity including but not limited to:

     a. Discrimination on the basis of race, creed, color, sex, age, national origin, martial status, religion, disability, sexual orientation, or veteran's status;

     b. Harassment, sexual or otherwise;

     c. Copyright infringement; or

     d. Expression of an employee's personal political beliefs or personal business interests.

   - Electronic communications resources are limited and employees must manage their allotted resources in a responsible manner. This includes but is not limited to deleting old messages and downloading e-mail messages to diskettes for long-term storage.

4. **All agency information technology resources, including electronic messaging systems and files, are the property of the state of Washington.**

   - The Department may, under certain circumstances and in the course of normal business functions, access an employee's electronic messages without authorization from the employee.

5. **Electronic messages sent globally (e.g., to "*ALL") must be appropriate for type and content. Examples of appropriate global messages are those that pertain to normal operations of the Department such as training and security alerts.**

6. **Communications media shall be managed in conformance with statutes and rules.**

   - Management of the Department's electronic communications media shall conform to all applicable statutes and regulations governing public records, records retention and public disclosure.

APPENDIX D

SAMPLE - Agency's E-mail Guidelines

Purpose. This document provides guidance regarding record status, retention, and management of electronic mail (email) messages. Organizing and managing email (and other electronic files) will save space, provide more efficient access, maintain confidentiality where needed, and reduce legal exposure in "discovery" proceedings.

Electronic Mail. Email is just another type of public record. Formally, it is a document created or received on an electronic mail system, which includes brief notes, more formal or substantive documents, and any attachments that may be transmitted with the message.

Messages and attachments should be filed and retained according to the legal retention required for the informational content of each (see Retention below). To assure appropriate retention of public records generated or received through and email system, it is recommended that you transfer messages and attachments to paper, disk, or LAN (network) drive.

Public Records. Public records are defined (per RCW 40.14.010) as "..."public records" shall include any paper, correspondence, completed form, bound record book, photograph, film, sound recording, map drawing, machine-readable material, or other document, regardless of physical form or characteristics, and including such copies thereof, that have been made by or received by any agency of the state of Washington in connection with the transaction of public business..."

Back-up. Email should be considered a communication tool, not a storage mechanism. Back-ups are for disaster recovery purposes only. Retention is the responsibility of the sender and receiver of the message, not the back-up process. Back-up copies performed by Information Technology staff are NOT records retention.

Confidentiality. Confidential and sensitive information should not be sent via email. The privacy and integrity of an email message cannot be guaranteed. Also, once created, there is no guarantee that attempts to erase or delete email will be effective.

Privacy. All messages originated or transported within or received in the email system are considered the property of the agency. If requested by a member of the public, email will possibly be released. For further information, see the Public Records Act (RCW 42.17.250 et seq.), and the Ethics Board WAC (292-110-010), and *reference your agencies public disclosure policy*. Tape or disk copies of deleted documents are also subject to the Public Records Act.

Legal Proceedings. Like other forms of records, and regardless of retention requirements, email pertaining to pending audits, or judicial or public disclosure proceedings must not be destroyed until the issue is resolved.

Retention. Email messages are subject to the guidelines in RCW 40.14 regulating the preservation and destruction of public records and as such are managed through records retention schedules. Email that is considered to have no administrative, legal, fiscal, or archival requirements for its retention may be deleted as soon as it has served its reference purpose.

- □ **Duplicates:** Extra copies of correspondence, completed forms, bulletins, statistics, reports, hardcopy printouts from a database, electronic files extracted from a master file or database, mailing lists, etc., used only for reference of informational distribution

- □ **Document Errors:** Incorrect versions of documents, forms or reports that had to be regenerated in order to correct errors in typing data entry, spelling, grammar, or format.

- □ **Miscellaneous Notices or Memoranda:** Memos and postings that do not related to the functional responsibility of the department (i.e., announcements of meetings, reservations, confirmations, itineraries, acknowledgements, form-letter thank you notes, etc.).

- □ **Preliminary Drafts:** Drafts of memos, letters, reports, worksheets, etc., that represent stylistic, spelling or grammatical changes.

- □ **Published Reference Materials:** Printed materials received from other offices, vendors, or others, which require no action and are not needed for documentary purposes. May include technical reports/studies, magazines, catalogs, periodicals, flyers, announcements, newsletters, and other widely distributed printed materials received.

- □ **Requests for Information:** Routine memos or forms used to request, or respond to requests for information, forms, mailing lists, database printouts, publications, etc. Retain until after the information has been sent or received.

- □ **Routing Slips:** Memos used to direct the distribution of documents.

- □ **Stocks of Publications:** Supplies (multiple copies) of departmentally produced printed documents, which are superseded, obsolete, or otherwise valueless. May include program brochures, booklets, flyers, forms, catalogs, directories, manuals, posters, and other informational materials produced by a department for wide distribution.

- □ **Transmittal Memos:** Letters and FAX cover sheets, which accompany a document, report, form, etc., that do not add any substantive information to the transmitted material.

The following categories of messages have specific retention periods. Some samples have been included but they are not inclusive. Refer to the state general records retention schedules[4] (available on the internet at http://www.secstate.wa.gov/archives/gs.aspx), or contact your agency Records Officer/Coordinator to determine the general or unique record series you are using.

For the email records that have not met their retention period, they should be printed to paper or disk and filed appropriately. Those that have met retention requirements should be deleted. *For public records with a retention period of more than three years, producing a paper copy for filing purposes is recommended to eliminate possible migration problems.*

Policy and Procedure Directives:

- Executive Level (GS 10 002) Administrative policies and procedures issued at the executive level of an agency to address agency-wide operations, critical agency functions, or issues of public visibility or concern. May

[4] *NOTE: This sample refers to a State Agency. Local Governments need to reference their specific general schedules and appropriate retentions.*

include formal directives, formal policy statements, printed or published procedures manuals, bulletins, orders, rules, or notices. *NOTE: Does not apply to policies and procedures, which regulate activities outside the agency or ones that are established through statute or through Washington Administrative Code (WAC) procedures.* **Retention: 6 years after superseded – ARCHIVAL**

- Routine General Office Polices and Procedures (GS 09 001): Polices and procedures covering the routine, day-to-day operations of an office or unit. *NOTE: Does not include agency mission-related policies and procedures – see GS 10 002 above.* **Retention: Destroy when superseded.**

Correspondence or Memoranda Related to Official Public Business:

- Executive Level (GS 10 007) Correspondence and memos at the executive level, to and from public officials, the public, and others, concerning policy issues, concerns, actions, or issues. **Retention: 4 years – Archival**
- Routine Correspondence (GS 09 005): concerning day-today office administration and activities. Includes correspondence between other offices within an agency, routine correspondence with other agencies, and correspondence with the public on routine matters. *Note: Does not apply to program level records. Refer to your office records retention schedule or contact you agency records officer.* **Retention: 30 days**

Agendas and Minutes of Meetings:

- Administrative Subject Files and General Documentation (GS 10 003) Executive level documentation of the administration of agency activities. May include minutes of meeting, management team meeting minutes, agendas, organizational charts, narrative reports, reports from agency divisions and sub-divisions, studies, news releases, newspaper clippings, correspondence, and other materials. *NOTE: Does not apply to program level records. Refer to your office records retention schedule or contact you agency records officer.* **Retention: 4 years - Archival**

- Governing Body Meeting Files and Minutes (GS 10 004): Minutes and meeting files of the governing body of an agency, such as Boards, Commissions, Councils, if the agency is so governed. **Retention: 2 years**

- Minutes and Files of Program Meetings (GS 09 010): Minutes, agendas, and meeting files from agency staff meetings, internal committees, task force committees, and other internal agency meetings which meet to coordinate activities, work out problems, serve as sounding boards, or vehicles of communications. **Retention: 2 years**

- Minutes and Files of Policy-Setting Meetings (GS 09 010): Minutes, agendas, and meeting files from meetings, which formulate policy, rules, or regulations for an agency or a number of agencies. *NOTE: Does not include program meetings or governing body meetings.* **Retention: 6 years - Archival**

- Documents Relating to Legal or Audit Issues: refer to the State General Schedule
  - FISCAL & ACCOUNTING OPERATIONS (GS 01),
  - AGENCY FINANCIAL REPORTING SYSTEMS (GS 02)

- COMBINED ANNUAL FINANCIAL REPORTS (GS 04)
- LEGAL FILES (GS 18)

Also, refer to your office specific/unique records retention schedule for your office. If you still don't know, contact your records coordinator or agency records officer.

- Program Specific Records*: You may include examples of your agencies program files (e.g. medical records with a ten year retention, client files, applications for licensing) and a statement to refer to your office Records Retention Schedule that is available from your Records Coordinator – include a list of Records Coordinator's and the Records Officer attached.* Following are some examples of program specific records:

  a. Messages which document departmental/office actions, decisions, operations, and responsibilities:
  b. Documents that initiate, authorize, or complete a business transaction.
  c. Drafts of documents that are circulated for comment or approval.
  d. Final reports or recommendations:

  Retention: Refer to the State General Schedules and your office Records Retention Schedules

Appointment Calendars:

- Executive Calendars (GS 10 008): A record of appointments, "to do" lists, and meeting schedules. Provides a day-by-day record of official activities.
  If maintained in electronic form the information should be printed out as often as necessary to provide a daily record. **Retention: 4 years – Archival**

- Calendars, Appointment Books, Routine Telephone Logs: A record of employee appointments, schedules, meetings, visitors, routine phone call logs, etc. **Retention: 1 year**

- Email Distribution Lists (GS 09 002): Part of office reference files **Retention: Destroy when no longer needed.**

- Other Messages Sent or Received that Relate to the Transaction of Agency Business. **Retention: Refer to the State General Schedules and your office Records Retention Schedules**